UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/784,440	02/23/2004	Hashem Mohammad Ebrahimi	1565.068US1	2576

21186 7590 05/11/2011

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2431	

NOTIFICATION DATE	DELIVERY MODE
05/11/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@slwip.com
request@slwip.com

Office Action Summary	Application No.	Applicant(s)	
	10/784,440	EBRAHIMI ET AL.	
	Examiner	Art Unit	
	KAVEH ABRISHAMKAR	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8,11-25,27 and 28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8,11-25,27 and 28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/28/2011*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication filed on February 28, 2011.

2. Claims 1-6, 8, 11-25, and 27-28 are currently pending consideration.

Information Disclosure Statement

3. An initialed and dated copy of Applicant's IDS (form 1449), received on February 28, 2011, is attached to the Office Action.

Priority

1. The instant application is a continuation in part to application 10650211. The parent application does not disclose any embodiments that feature all limitations of each of the instant claims. For example, none of a forward proxy, reverse proxy and/or transparent proxy are identified as embodiments in the earlier application. Hence, the priority date with respect to the prior art for the instant claims of this application is the filing date of the instant application. See amended specification filed on 1/21/09.

Claim Interpretation

2. With respect to the following limitation of claim 1 ("the remote site delegates data vending on behalf of the remote site to be managed and distributed by the local managing service from within the local processing environment of the client and the local managing service presents itself to the client as the remote site"), the disclosure on pg. 7 of Applicant's specification is deemed pertinent:

> Thus, when the proxy 102 detects that a client 101 is attempting to establish secure communications with a remote site 120 that is associated with a particular local managing service 103, the proxy 102 passes the client 101 request for 10 communication along to the particular local managing service 103. The local managing service 103 is trusted by the remote site 120, this means that the remote site 120 may house the identity of the local managing service 103 in one of its trusted data stores which identifies trusted parties. The remote site 120 also recognizes communications with the local managing service 103 as being secure. 15 Similarly, the local managing service 103 recognizes and trusts the remote site 120. Thus, the remote site 120 delegates its authority to the local managing service 103 to vend some of its data on behalf of it within the local networking environment of the client 101.
>
> One technique for doing this is to provide a digital certificate of the remote 20 site 120 to the local managing service 103. Typically, the remote site 120 provides certificates to trusted parties for purposes of decrypting its data communications. The remote site 120 may also provide an encryption key to the local managing service 103. The encryption key is what the remote site 120 personally uses to encrypt its data communications for purposes of secure communications with a 25 trusted party. Armed with the certificate and/or encryption key, the local managing service 103 can present itself to the client 101 within the client's local computing environment as if the local managing service 103 were in fact the remote site 120.
>
> Once the proxy 102 and the local managing service 103 are properly configured within the client's local computing environment, data can be managed 30 and accelerated by the local managing service 103 on behalf of the remote site 120 in the following manners.

3. With respect to the limitation "a local computing environment," the specification describes the proxy (reference no. 102) and local service (reference no. 103) depicted in fig. 1 as being "within the local computing environment of the client 101." See pg. 8, lines 27-31 and pg. 10, lines 9-15. Fig. 1 depicts the proxy (on a first server device), local service (on a second server device) and client (on a laptop) as devices situated

within a local network environment. Hence, “a local computing environment" as used in the claims appears to be analogous to a "local networking environment." On pg. 4 of the specification, Applicant provides a description of a “local networking environment,” which is reprinted here:

> Local networking environment refers to physical or logical network devices and services which are configured to be local to the clients and which interface with the clients. This does not mean that any particular local networking environment of a particular client physically resides in the same geographic location of the client or proximately resides within the same geographic location of the client, although in some embodiments this can be the case. *Local networking environments can be dispersed geographically from the physical location of the client and form a logical local networking environment of the client*. [Emphasis added]

4. This page of the Specification further discloses that "[a]n external networking environment is a network which is not considered local to the client.” In view of this portion of the specification, a device or service is “within a local computing environment” of a client if it forms a *logical local networking environment* of the client regardless of the geographic location of the client and the device or service. In other words, whether a device is within the “local computing environment” of the client depends solely on the operational relationship between the device and the client.

Response to Arguments

Applicant's arguments filed on February 28, 2011 have been fully considered but they are not persuasive for the following reasons:

The Applicant argues, on Page 10 of Remarks, that the Cited Prior Art (CPA) does not teach that a determination is made to process a local service within a local

environment of a client based on an identity for a particular remote site that a particular client is trying to access. This argument is not found persuasive. Boneh, US 2004/0015725, teaches a web proxy which is situated between a client and a web server (paragraph 0045). The client is trying to gain access to the web server and the proxy acts as an intermediary between them (paragraph 0045). This proxy is based on the identity of the remote site because the proxy inserts the destination name into its own certificate, and therefore, it is based on the identity of the remote site (paragraph 0045).

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. Claims 1-6, 8, 10-25, 27 and 28 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 3-15, 17-22 and 24-26 of copending Application No. 10814983. Although the conflicting claims are not identical, they are not patentably distinct from each other because the claimed method and system for managing and accelerating the delivery of data as defined in the instant claims are substantially defined in claims 1, 3-15, 17-22 and 24-26 of copending Application No. 10814983.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-6, 8, 11-25, 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh et al. US 20040015725 (hereinafter Boneh) in view of Aziz et al. US 6,643,701 (hereinafter Aziz).

9. As per claims 1-6, Boneh discloses a method for managing and accelerating the delivery of data implemented in a computer-readable storage medium and processed on a proxy device for performing the method, comprising:

a. receiving a secure communications request for data associated with a remote site, wherein the request is received from a client and the secure communications request occurs via Secure Socket Layer (SSL) communications with the client (paragraph 26) and wherein the request is received at a forward proxy that processes within a local processing environment of the client (fig. 4; paragraph 36, browser first sends a message CONNECT www.xyz.com to the web proxy; compare with paragraph 47, where no CONNECT messages is pre-appended);

b. processing a local managing service from within a local computing environment of the client (see fig. 4, the proxy server is situated locally with the client and forms a logical local networking environment of the client)

c. determining that a local managing service is needed to mediate between the client and the remote site based on an identity for the remote site (paragraph 0045).

d. passing the request to the local managing service for processing acting as the forward proxy for the client, wherein the local managing service is capable of caching the data for servicing the secure communications request of the client within the local processing environment of the client and capable of securely interfacing with the remote site (paragraphs 34-42; client sends the connect

request message to the web proxy; proxy performs caching on decrypted response);

e. the local managing service houses an identity for the remote site and local managing service is trusted by the remote site and the remote site delegates authority to the local managing service to vend data of the remote sites within the local processing environment of the client (paragraphs 37 and 41, web proxy creates a TLS session to the site www.xyz.com; TLS session establishment entails certificate exchange and verification between the web proxy and the remote site; see also pg. 7, lines 13-18 of the instant specification);

f. creating, by the local proxy device, a secure communications tunnel between the client and the local managing service (paragraph 40, TLS session between the client and the web proxy; see for example paragraph 12 for TLS session generation); and

g. creating, by the proxy device, another secure communications tunnel between the local managing service and the remote site (paragraph 41, web proxy creates a TLS session with the site www.xyz.com);

h. determining, by the local managing service, when the secure communications request can be satisfied with cached data; and supplying the data from the cached data to the client with secure communications, when present in cache; requesting, by the local managing service, the data from the remote site if the data is not in the cache; receiving the data from the remote site; and supplying the data to the client with secure communications; housing the

data in the cache for subsequent requests made by the client or other clients for the data, when the data is permitted to be cached (paragraph 42, all features are inherent in caching services);

i. maintaining, by the local managing service, a certificate associated with communications from the remote site (paragraph 41);

j. transmitting, by the local managing service, to the remote site a first certificate associated with the identity of the local managing service;

receiving, from the remote site, at the local managing service a second certificate associated with the identity of the remote site; and communicating between the remote site and the local managing service with Secure Sockets Layer (SSL) communications using the first and second certificates (paragraph 41).

10. Furthermore Boneh discloses that the web proxy presents itself to the client as the remote site by generating a server certificate at the web proxy and communicating the certificate to the user client. Secure communications between the client and the web proxy is established using the key inserted into the certificate (paragraph 45, “the browser is configured to accept this proxy-server certificate, the web proxy successfully binds the destination server name (www.xyz.com) to the proxy-generated proxy session public key, allowing the proxy to thereafter masquerade as the destination server www.xyz.com”)

11. Boneh does not expressly disclose that the local service acts as a reverse proxy on behalf of the remote site from the local processing environment of the client, whereby the remote site delegates data vending on behalf of the remote site to be

managed and distributed by the local managing service from within the local processing environment of the client. Aziz discloses a method and apparatus for providing secure communications between a client and a server. When the client desires to establish a secure connection with the remote server, a first secure communication is established between the client and a relay, and a second secure communication is then established between the relay and the server. In particular, on col. 5, lines 1-22 and col. 8, lines 13-32, Aziz discloses

> Information stored on relay 220 is used to create the secure connection. When a server wishes to obtain advantages of the present invention in a manner that could be transparent to client 200, server 240 will have a trust relationship with (that is, be controlled by or even be owned by the same entity as) relay 220. Therefore, server 240 will share its private key and certificate with relay 220. When a client wishes to obtain advantages of the present invention in a manner that could be transparent to server 240, client 200 will have a trust relationship with relay 220, and client 200 will, e.g., accept the certificate of relay 220 as that of server 240 and provide an authentication token of client 200 to relay 220. Thereby, relay 220 may be inserted without access to the server's keys. This architecture could, for example, assist a programmer in diagnosing problems with a client's application that communicates with an HTTPS server (by convention a secure server address is given the prefix "https://") even when the server would not provide the programmer with access to the server's keys. When both client 200 and server 240 wish to achieve the advantages of the present invention in a manner known to each entity, each will provide appropriate information to relay 220. …
>
> …Because relays 320 are trusted by server 340, server 340 provides each relay 320 with its security certificate and with its public and private key pair for use in an encryption/decryption process (step 910). Either prior to during, or in response to a client request for information from server 340, the secure connection program of relay 320 and the secure connection program of server 340 create an end-to-end security link 330 using a handshaking session (step 920). For example, using SSL, this link is established following a handshaking session similar to that described with regard to FIG. 1. For enhanced security, each end point (relay and server) authenticates one another using the relay's certificate and private/public key pair and the server's certificate and private/public key

> pair. The secure connection program of relay 320 and the secure connection program of server 340 could also create link 330 following a refresh handshaking session that occurs after an initial handshaking session. The refresh handshaking session could occur at a predetermined period based on an elapse of a predetermined time, transfer of a predetermined amount of information, etc. to provide replacement session keys and, thus, increased security.

12. It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Boneh such that that the local service acts as a reverse proxy on behalf of the remote site from the local processing environment of the client, whereby the remote site delegates data vending on behalf of the remote site to be managed and distributed by the local managing service from within the local processing environment of the client. One would be motivated to do so to avoid performing intensive processing tasks such as generating private keys and digital certificates at a network juncture as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 1-6.

13. As per claims 8 and 11-15, Boneh discloses a method of managing and accelerating delivery of data implemented in a computer-readable storage medium and to process within a local networking environment of a client for performing the method, comprising:

k. processing a local service of a proxy for communicating securely with the client and for acting on behalf of the client during interactions between the client and a remote site (fig. 4), wherein the local service processes from within a local computing environment of the client and uses Secure Socket Layer (SSL)

communications when interacting with the client (paragraph 26); managing authority from the remote site at the local service and within the local computing environment of the client (see fig. 4, the proxy server is situated locally with the client and forms a logical local networking environment of the client; paragraphs 37 and 49);

l. establishing a secure tunnel between the local service of the proxy and the client for interactions between the client and the local service (paragraph 51, secure TLS session between the client and the web proxy);

m. establishing another secure tunnel between the local service and the remote site for interactions between the local service and the remote site (paragraph 53, secure TLS session between the web proxy and the remote site); and

n. caching, within the local service, data received from the remote site, and wherein portions of the data are sent to the client in order to service data requests made from the client to the remote site (paragraphs 46-54);

o. initially transmitting a local service certificate to the remote site; and subsequently communicating securely between the local service and the remote site using the local service certificate and the certificate of the remote site (paragraph 53);

p. establishing the proxy as a transparent proxy for the client (paragraph 47);

q. inspecting at the proxy a secure request made from the client for the remote site; and transferring the secure request to the local service for processing (paragraph 52);

r. wherein caching further includes housing the data in a decrypted format within cache of the local service (paragraph 54, caching services are performed on decrypted response);

s. wherein caching further includes sending the portions of the data from the cache to the client along with the certificate associated with the remote site (paragraph 49 and 54 [cache services]).

14. Furthermore Boneh discloses that the web proxy presents itself to the client as the remote site by generating a server certificate at the web proxy and communicating the certificate to the user client. Secure communications between the client and the web proxy is established using the key inserted into the certificate (paragraph 45, “the browser is configured to accept this proxy-server certificate, the web proxy successfully binds the destination server name (www.xyz.com) to the proxy-generated proxy session public key, allowing the proxy to thereafter masquerade as the destination server www.xyz.com”)

15. Boneh does not expressly disclose that the local service acts as a reverse proxy on behalf of the remote site from the local computing environment of the client, whereby the remote site delegates data vending on behalf of the remote site to be managed and distributed by the local managing service from within the local processing environment of the client; and that the authority is managed by accessing a certificate of the remote

site at the local service. Aziz discloses a method and apparatus for providing secure communications between a client and a server. When the client desires to establish a secure connection with the remote server, a first secure communication is established between the client and a relay, and a second secure communication is then established between the relay and the server. In particular, on col. 5, lines 1-22 and col. 8, lines 13-32, Aziz discloses

> Information stored on relay 220 is used to create the secure connection. When a server wishes to obtain advantages of the present invention in a manner that could be transparent to client 200, server 240 will have a trust relationship with (that is, be controlled by or even be owned by the same entity as) relay 220. Therefore, server 240 will share its private key and certificate with relay 220. When a client wishes to obtain advantages of the present invention in a manner that could be transparent to server 240, client 200 will have a trust relationship with relay 220, and client 200 will, e.g., accept the certificate of relay 220 as that of server 240 and provide an authentication token of client 200 to relay 220. Thereby, relay 220 may be inserted without access to the server's keys. This architecture could, for example, assist a programmer in diagnosing problems with a client's application that communicates with an HTTPS server (by convention a secure server address is given the prefix "https://") even when the server would not provide the programmer with access to the server's keys. When both client 200 and server 240 wish to achieve the advantages of the present invention in a manner known to each entity, each will provide appropriate information to relay 220. …
>
> …Because relays 320 are trusted by server 340, server 340 provides each relay 320 with its security certificate and with its public and private key pair for use in an encryption/decryption process (step 910). Either prior to during, or in response to a client request for information from server 340, the secure connection program of relay 320 and the secure connection program of server 340 create an end-to-end security link 330 using a handshaking session (step 920). For example, using SSL, this link is established following a handshaking session similar to that described with regard to FIG. 1. For enhanced security, each end point (relay and server) authenticates one another using the relay's certificate and private/public key pair and the server's certificate and private/public key pair. The secure connection program of relay 320 and the secure connection program of server 340 could also create link 330 following a

refresh handshaking session that occurs after an initial handshaking session. The refresh handshaking session could occur at a predetermined period based on an elapse of a predetermined time, transfer of a predetermined amount of information, etc. to provide replacement session keys and, thus, increased security.

16. It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Boneh such that the web proxy acts as a reverse proxy on behalf of the remote site from the local computing environment of the client, whereby the remote site delegates data vending on behalf of the remote site to be managed and distributed by the local managing service from within the local processing environment of the client; and that the authority is managed by accessing a certificate of the remote site at the local service. One would be motivated to do so to avoid performing intensive processing tasks such as generating private keys and digital certificates at a network juncture as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 8 and 11-15.

17. As per claim 16-22, Boneh discloses a data management and acceleration delivery system implemented in computer-readable storage media and to process on devices of a network, the system comprising:

t. a proxy; a local service accessible to the proxy; and a remote site external to the proxy, wherein the proxy directs secure requests received from a client for the remote site to the local service (fig. 4), the local service: acts as a transparent proxy on behalf of the client, processes within a local computing environment of the client (reference no. 352, the proxy server is situated locally with the client

and forms a logical local networking environment of the client), and communicates securely with the client using Secure Socket Layer (SSL) communications (paragraph 26) via a first secure tunnel established by the proxy for interactions between the local service and the client, and the local service interacts securely with the remote site via a second secure tunnel established by the proxy for interactions between the local service and the remote site, the interactions between the local service and the remote site is to acquire data on behalf of the client, and wherein portions or all of the acquired data are cached within the local service and used to service requests made by the client from within the local computing environment of the client (paragraphs 46-54; in particular, in paragraph 51, secure TLS session between the client and the web proxy is established, and in paragraph 53, secure TLS session between the web proxy and the remote site is established);

u. wherein the local service includes a certificate with an identity of the remote site which is vended to the client (paragraphs 37 and 49);

v. wherein the local service and remote site mutually interact securely with one another by exchanging certificates with one another (paragraph 53);

w. wherein the local service and the remote site sign communications occurring between them (in SSL client authentication and key exchange is performed via signature);

x. wherein the client is a browser application (paragraph 46);

y. wherein the browser is configured to contact the proxy when making requests directed to the remote site (paragraph 48);

z. wherein the proxy intercepts requests made from the browser which are directed to the remote site and forwards the requests to the local service for handling the requests (paragraph 46).

18. Furthermore Boneh discloses that the web proxy presents itself to the client as the remote site by generating a server certificate at the web proxy and communicating the certificate to the user client. Secure communications between the client and the web proxy is established using the key inserted into the certificate (paragraph 45, "the browser is configured to accept this proxy-server certificate, the web proxy successfully binds the destination server name (www.xyz.com) to the proxy-generated proxy session public key, allowing the proxy to thereafter masquerade as the destination server www.xyz.com")

19. Boneh does not expressly disclose that the local service is also configured for acting as a reverse proxy on behalf of the remote site from the local computing environment of the client, whereby the remote site delegates data vending on behalf of the remote site to be managed and distributed by the local managing service from within the local processing environment of the client. Aziz discloses a method and apparatus for providing secure communications between a client and a server. When the client desires to establish a secure connection with the remote server, a first secure communication is established between the client and a relay, and a second secure

communication is then established between the relay and the server. In particular, on col. 5, lines 1-22 and col. 8, lines 13-32, Aziz discloses

> Information stored on relay 220 is used to create the secure connection. When a server wishes to obtain advantages of the present invention in a manner that could be transparent to client 200, server 240 will have a trust relationship with (that is, be controlled by or even be owned by the same entity as) relay 220. Therefore, server 240 will share its private key and certificate with relay 220. When a client wishes to obtain advantages of the present invention in a manner that could be transparent to server 240, client 200 will have a trust relationship with relay 220, and client 200 will, e.g., accept the certificate of relay 220 as that of server 240 and provide an authentication token of client 200 to relay 220. Thereby, relay 220 may be inserted without access to the server's keys. This architecture could, for example, assist a programmer in diagnosing problems with a client's application that communicates with an HTTPS server (by convention a secure server address is given the prefix "https://") even when the server would not provide the programmer with access to the server's keys. When both client 200 and server 240 wish to achieve the advantages of the present invention in a manner known to each entity, each will provide appropriate information to relay 220. …
>
> …Because relays 320 are trusted by server 340, server 340 provides each relay 320 with its security certificate and with its public and private key pair for use in an encryption/decryption process (step 910). Either prior to during, or in response to a client request for information from server 340, the secure connection program of relay 320 and the secure connection program of server 340 create an end-to-end security link 330 using a handshaking session (step 920). For example, using SSL, this link is established following a handshaking session similar to that described with regard to FIG. 1. For enhanced security, each end point (relay and server) authenticates one another using the relay's certificate and private/public key pair and the server's certificate and private/public key pair. The secure connection program of relay 320 and the secure connection program of server 340 could also create link 330 following a refresh handshaking session that occurs after an initial handshaking session. The refresh handshaking session could occur at a predetermined period based on an elapse of a predetermined time, transfer of a predetermined amount of information, etc. to provide replacement session keys and, thus, increased security.

20. It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Boneh such that that the local service is also configured to act as a reverse proxy on behalf of the remote site from the local computing environment of the client, whereby the remote site delegates data vending on behalf of the remote site to be managed and distributed by the local managing service from within the local processing environment of the client. One would be motivated to do so to avoid performing intensive processing tasks such as generating private keys and digital certificates at a network juncture as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 16-22.

21. As per claims 23-25, 27 and 28, Boneh discloses a data management and acceleration delivery system implemented in a computer-readable storage medium and to process on one or more devices of a network, the system comprising:

aa. a proxy; and one or more local services directly accessible to the proxy, wherein the proxy acts as an intermediary between one or more clients and one or more remote sites (fig. 4), the proxy detects attempts made by the clients for establishing secure communications with the remote sites and based on the identities of a particular client and particular remote site identifies a particular local service, the particular local service: communicates securely with the particular client via Secure Socket Layer (SSL) (paragraph 26) communications as a transparent proxy to the particular client and via a first tunnel established by the proxy between the particular local service and the particular client, the

particular local service processes within a local computing environment of the particular client, and the particular local service also securely communicates with the particular remote site via a second tunnel established by the proxy between the particular local service and the particular remote site, and wherein the particular local service caches data received from the particular remote site for purposes of servicing requests for portions of that data requested by the particular client and the cached data resides within the local computing environment of the particular client (paragraphs 46-54; in particular, in paragraph 51, secure TLS session between the client and the web proxy is established, and in paragraph 53, secure TLS session between the web proxy and the remote site is established; fig. 4, reference no. 352, the proxy server is situated locally with the client and forms a logical local networking environment of the client);

bb. wherein each local service is associated with a unique one of the remote sites (paragraph 31);

cc. further comprising switching logic that intercepts requests from the clients which are directed to the remote sites and forwards them to the proxy (paragraph 46);

dd. wherein each of the local services includes a certificate associated with a unique one of the remote sites; wherein a number of the local services communicates securely with a number of the remote sites by initially exchanging mutual certificates (the invention operates via SSL or TLS).

22. Furthermore Boneh discloses that the web proxy presents itself to the client as the remote site by generating a server certificate at the web proxy and communicating the certificate to the user client. Secure communications between the client and the web proxy is established using the key inserted into the certificate (paragraph 45, "the browser is configured to accept this proxy-server certificate, the web proxy successfully binds the destination server name (www.xyz.com) to the proxy-generated proxy session public key, allowing the proxy to thereafter masquerade as the destination server www.xyz.com")

23. Boneh does not expressly disclose that the particular local service acts as a reverse proxy on behalf of the remote site from the local computing environment of the client, whereby the remote site delegates data vending on behalf of the remote site to be managed and distributed by the local managing service from within the local processing environment of the client. Aziz discloses a method and apparatus for providing secure communications between a client and a server. When the client desires to establish a secure connection with the remote server, a first secure communication is established between the client and a relay, and a second secure communication is then established between the relay and the server. In particular, on col. 5, lines 1-22 and col. 8, lines 13-32, Aziz discloses

> Information stored on relay 220 is used to create the secure connection. When a server wishes to obtain advantages of the present invention in a manner that could be transparent to client 200, server 240 will have a trust relationship with (that is, be controlled by or even be owned by the same entity as) relay 220. Therefore, server 240 will share its private key and certificate with relay 220. When a client wishes to obtain advantages of the present invention in a manner that could be transparent to server 240, client 200 will have a trust relationship with relay 220, and client 200 will,

> e.g., accept the certificate of relay 220 as that of server 240 and provide an authentication token of client 200 to relay 220. Thereby, relay 220 may be inserted without access to the server's keys. This architecture could, for example, assist a programmer in diagnosing problems with a client's application that communicates with an HTTPS server (by convention a secure server address is given the prefix "https://") even when the server would not provide the programmer with access to the server's keys. When both client 200 and server 240 wish to achieve the advantages of the present invention in a manner known to each entity, each will provide appropriate information to relay 220. …
>
> …Because relays 320 are trusted by server 340, server 340 provides each relay 320 with its security certificate and with its public and private key pair for use in an encryption/decryption process (step 910). Either prior to during, or in response to a client request for information from server 340, the secure connection program of relay 320 and the secure connection program of server 340 create an end-to-end security link 330 using a handshaking session (step 920). For example, using SSL, this link is established following a handshaking session similar to that described with regard to FIG. 1. For enhanced security, each end point (relay and server) authenticates one another using the relay's certificate and private/public key pair and the server's certificate and private/public key pair. The secure connection program of relay 320 and the secure connection program of server 340 could also create link 330 following a refresh handshaking session that occurs after an initial handshaking session. The refresh handshaking session could occur at a predetermined period based on an elapse of a predetermined time, transfer of a predetermined amount of information, etc. to provide replacement session keys and, thus, increased security.

24. It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Boneh such that that the particular local service acts as a reverse proxy on behalf of the remote site from the local computing environment of the client, whereby the remote site delegates data vending on behalf of the remote site to be managed and distributed by the local managing service from within the local processing environment of the client. One would be motivated to do so to avoid performing intensive processing tasks such as generating private keys and digital

certificates at a network juncture as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 23-25, 27 and 28.

Conclusion

25. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

26. Bellwood et al. US 6,584,567 discloses a proxy establishing a secure communication between a client and a set of servers and further providing caching services.

27. Chawla et al. US 7,137,143 discloses a secure reverse proxy establishing separate secure connections between a client and a web server and further providing caching services.

28. "Secures Sockets Layer Discussion List FAQ v1.1.1," pg. 7 (entered 9/17/08) discloses establishing separate secure connections between a client and a Netscape Proxy server and between a Netscape Proxy server and an external server.

29. Ackaouy et al. US 7,552,223 disclose a method and system to provide active data from one or more storage servers to one or more clients by situating a proxy cache between the client and the storage servers. The proxy cache can be configured as either a forward proxy or reverse proxy. See col. 3, lines 32-38.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Primary Examiner, Art Unit 2431

/K. A./
05/06/2011
Primary Examiner, Art Unit 2431